(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: VIDEO/IMAGE COMMUNICATION WITH WATERMARKING
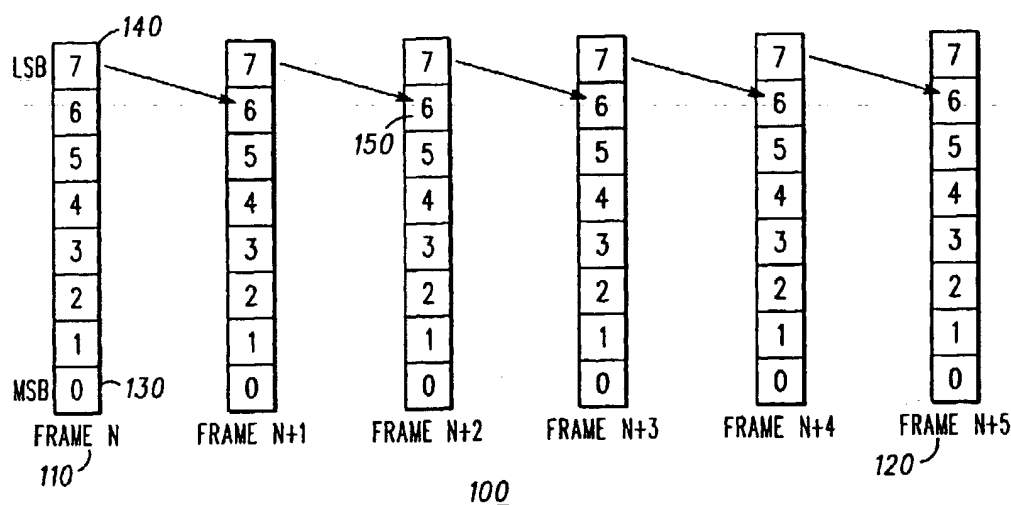
(57) Abstract: A video communication unit (405, 450) comprising a video input (415) for receiving a video signal transmission having a number of video or image frames, wherein each video or image frame includes a number of bit planes, the video input being operably coupled to a processor, the video communication unit characterised by said processor (410, 460) replicating at least one bit plane in at least two video or image frames to provide a tamper detection means of the video or image signal transmission. This enables fraudulent tampering of image and video to be detected, and the location of such tampering to be revealed to users of the material.

1

Video/Image Communication With Watermarking

Field of the Invention

5   This invention relates to video transmission systems and
related video encoding/decoding techniques. The invention
is applicable to, but not limited to, a video compression
system employing video watermarking where any tampering of
a video image or portion of video image is to be detected.
10

Background of the Invention

The ability to transmit real-time video and/or image data
is a desirable characteristic of many current wireline and
15   wireless communication systems. However, it is known that
individual images/pictures, or a series of images say, in
a transmitted video stream, may be subjected to 'attacks',
i.e. the images may have been tampered with. Therefore, a
need exists to protect image or video transmissions from
20   such undesirable tampering. One known technique employed
to protect still/video images or documents is by the use
of "watermarks".

In the context of the present invention, the terms 'video'
25   and 'image' are used interchangeably, with the term
'video' generally used to represent one or more still
images.

Wolfgang R, Podilchuk C, Delp E "Perceptual watermarks for
30   digital images and video", SPIE Conference on Security and
Watermarking of Multimedia Content, January 1999,
describes some state of the art watermarking methods for
use with video and images.

2

Protection of digital media (including image and video) has also become a key standardisation topic within the multimedia industry over the last year. Police users have

5   formally stated that they do not envisage using digitally transmitted and processed images for evidential purposes without the existence of reliable tamper detection methods.

10 The European Broadcasting Union has issued a second call for systems that offer watermarking of multimedia transmissions for entertainment applications. In addition, the International Standards Organisation (ISO) has set up a working group known as MPEG-21, whose

15 essential function is to investigate digital rights management including the authentication of multimedia data.

In image watermarking, a known binary pattern or signature

20 is embedded into an image at the moment of image acquisition. Such watermarks are termed "robust", because they are designed to remain intact regardless of any post-processing of the image such as filtering, cropping, etc.

25 While such watermarks do provide a useful degree of protection, they cannot at present be wholly relied on in a court of law. The purpose of these watermarking methods is such that they are not designed to possess the required degree of surety that an image has not been tampered with,

30 in order for the image to be used as evidence.

Thus, there exists a need in the field of the present invention to provide a video communication unit and

methods, based on a watermarking system, that can be used
for testing a video sequence for evidence of tampering,
wherein the abovementioned disadvantages may be
alleviated. Furthermore, there exists a need for a
5 labelling method to highlight areas of a video sequence
that are detected as having been tampered with.
Additionally, it would be beneficial to visually label
tampered video sequences such that they are rendered
unusable, or valueless, to the attacker.
10

Published prior art documents include:
(i) US-A-5875249 (Mintzer et al.);
(ii) 'Digital watermarking through quasi m-arrays', YEH et
al., IEEE conference proceedings 29 November 1999, pages
15 459-461;
(iii) 'A digital watermark', OSBORNE et al., IEEE
conference proceedings 13-16 November 1994, pages 86-90.

Statement of Invention
20

The present invention provides video communication units,
a video transmission system adapted to use one of the
video communication units, a mobile radio device, a method
of watermarking a video signal transmission in a video
25 transmission system, a method of detecting tampering of a
watermarked digital image, a method of visually labelling
a video sequence that contains an attacked watermark, a
storage medium storing processor-implementable
instructions for controlling a processor to carry out any
30 of the methods of the invention, a video communication
unit adapted to perform any of the methods of the
invention, a mobile radio device, all as claimed in the
appended independent claims.

4

Brief Description of the Drawings

Exemplary embodiments of the present invention will now be
5   described, with reference to the accompanying drawings, in
which:

FIG. 1 shows a watermark embedding method, in accordance
with the preferred embodiment of the invention.

FIG. 2 shows a method of detecting frames that have been
10 tampered with, in accordance with the preferred embodiment
of the invention.

FIG. 3 shows a flowchart of a decision process for
determining whether tampering has occurred, in accordance
with the preferred embodiment of the invention.

15 FIG. 4 shows a block diagram of a video communication
system incorporating a communication unit embedding a
watermark, and a communication unit detecting a watermark,
in accordance with the preferred embodiment of the
invention.

20

Description of Preferred Embodiments

The inventive concepts described herein find particular
application in the current MPEG Standards activities,
25 where a standard watermarking system for video use is to
be defined. The detection of tampering, and the ability
to determine what type of tampering has taken place, are
necessary steps in ensuring user confidence in the images
and video sequences a user is viewing in a potentially
30 hostile multimedia communication environment.

In summary, the preferred embodiment of this invention
aims to pre-process video material such that detection of
tampering can take place.

5   Most current image and video watermark methods focus on
pre-processing video and images such that any embedded
watermark can be recovered, regardless of tampering, for
example in copyright applications. The method described
below, however, provides for 'fragile' watermarks that are
10   destroyed when the images are altered.

Furthermore, the method makes clear that content has been
tampered with such that the person carrying out the
unauthorised processing realises that their actions are
15   evident. As a consequence, they cannot re-sell or
distribute the video as an "original".

As an example, let us consider a person making "pirated"
video files for unauthorised distribution via an internet
20   web site. The preferred method, as described below,
identifies where the video had been tampered with (e.g. in
reformatting the video for web distribution) and applies a
label to the tampered area, thereby rendering the video
unsuitable for onward distribution.

25

The preferred embodiment of the present invention can be
applied to video sequences consisting of at least two
image frames. Furthermore, the preferred embodiment of
the present invention can be applied to image formats

30   including YC_bC_r (a standard representation of a colour

image as specified in ITU Rec 601), red/green/blue (RGB),
or any single component (e.g. Y only) of an image format
consisting of more than one component. Advantageously,

the preferred embodiment of the present invention can also
be applied in a restricted area or region of an image, or
throughout the entire image.

5   The watermark arrangement of the preferred embodiment of
the invention clearly shows when tampering has occurred,
as tamper evident information is embedded into the video
data stream. In summary, the method facilitates
replication of bit planes in consecutive frames.

10
Furthermore, the method allows the video player to locate
the exact spatial and temporal position of the tampering
as the video is being played.

15   Referring first to FIG. 1, a watermarking method 100 is
shown, in accordance with the preferred embodiment of the
invention. The watermarking method 100 includes a
sequence of video/image frames - frame 'N' 110 to frame
'N+5' 120. Six frames are shown for clarity purposes

20   only. Each video/image frame includes a number of data
bits, ranging from a most significant bit plane (MSB) –
'bit 0' 130 to a least significant bit plane (LSB) – 'bit
7' 140. Again, each frame is shown as having eight bit
planes for clarity purposes only.

25
The usual representation of image data is as a series of
pixels, located as rows and columns of an image. Common
image formats include representation of each pixel in a
number of bits, from 6 to 12 bits per component of the

30   image. As an example, each single component (R, G or B)
of a colour image may have 8 bits per pixel, an infrared
image may have 12 bits per pixel represented as a
luminance component.

A "bit plane" representation is the term given to the
collection of individual bits at any one-bit position of a
pixel across the entire image. As an example, consider an
5   image or image region of size k columns and j rows, with
'N' bits per pixel. Each of the (k*j) pixels has 'N'
bits, which are ordered from a least significant bit (LSB)
usually termed bit 'N-1', up to a most significant bit
(MSB) termed bit 0.

10

A bit plane is a representation of the collection of (k*j)
bits considered at one bit position P, where $0<=P<=(N-1)$.
Thus the expression "the most significant bit plane" means
that we consider the collection of all bit 0's of all
15   (k*j) pixels in an image or image region. For an image
comprising 'N' bits per pixel, there will be 'N' bit
planes.

It is within the contemplation of the invention that a
20   video/image transmission system having any number of
frames in a sequence of video/image frames, including any
number of bit planes more than two, would benefit from the
inventive concepts described herein.

25   In the preferred embodiment of the invention, a 7th bit
plane (the LSB) 140 of a previous frame is moved into a
6th bit plane 150 of a current frame, assuming an 8 bit
per pixel image component, which is a common image format.
Clearly, it is not essential that the bit plane be moved
30   to the next least important bit-plane. However, the more
important the bit plane that is replaced, the larger the
adverse affect on the quality of the video transmission.

The 7th bit plane (the least significant bit-plane) 140
from the previous frame is placed in the 6th bit plane 150
of the current frame on a pixel-by-pixel basis. This
process repeats throughout the sequence, as illustrated in
5   FIG. 1.

As the 6th and 7th bit planes contain the least
significant portions of the video/image data, they can be
viewed as essentially noise. Such noise is imperceptible
10   to the human visual system. Thus, the inventors of the
present invention have recognised the benefits of using
such 'noise' as a form of tamper detection, in utilising
the replication of bit planes without producing any
noticeable artefacts in the image. As the 7th (LSB) bit
15   plane 140 is used, very small alterations in the pixel
values of the frame (±1) allow any tampering to be
detected.

It is noteworthy that for improved robustness to attack
20   and reduced disturbance to the original image, a subset of
pixels in a frame may be chosen for this process, in
contrast to using the entire video/image frame.

Referring next to FIG. 2, a method 200 of detecting which
25   frame has been tampered with is shown, in accordance with
the preferred embodiment of the invention.

FIG. 2 shows two video/image sequences:
(i)   an un-tampered sequence of frames 250, from a
30   frame 'N-2' 255 to a frame 'N+2' 260; and
(ii)   a tampered sequence of frames 210, from a frame
          'N-2' 215 to a frame 'N+2' 235.

9

Frame 'N' 225 is shown as having being tampered with. In order for the video player to test the video sequence, it extracts the 7th bit plane from the previous frame 'N-1' 220 and compares it on a pixel-by-pixel basis with the 6th

5   bit plane from the current frame 'N' 225. Any points within the two bit planes that do not match up indicate tampering at those pixels within the tampered frame 'N' 225. The location of the tampered frame, i.e. whether the tamper occurred in the current frame or previous frame,

10 can also be found using the method illustrated in FIG. 3.

As an example, consider the un-tampered sequence 250. Comparison of the 7th bit plane of the previous frame with the 6th bit plane of the current frame would reveal no

15 differences, to the bit plane content, on a pixel-by-pixel basis. However, in the tampered sequence 210, if the 6th bit plane of the current frame 'N' 225 does not exactly match the 7th bit plane of the previous frame 'N-1' 220, for some of the pixels in frame 'N' 225 of a sequence,

20 then we know tampering has occurred. This could be in frame 'N' 225 or frame 'N-1' 220. In this case, a further test is performed.

The 7th bit plane of frame 'N' 225 is compared with the

25 6th bit plane of frame 'N+1' 230 for those pixels believed to have been tampered. If the bit planes for those pixels between those frames are equal, then the tampering is known to have occurred in frame 'N-1' 220. If the bit planes for those pixels between those frames are not

30 equal, then the tampering is known to have occurred in frame 'N' 225.

By utilising the least significant bits or bit planes of a video/image transmission in this manner, an effective means of watermark embedding and tamper detection has been provided.

5

Referring now to FIG. 3, a flowchart 300 of a decision process for determining whether tampering has occurred is illustrated. As mentioned, a bit-wise comparison of the 6th bit plane of the current frame is made with the 7th bit

10 plane of the previous frame, as in step 302. If the comparison yields a match, namely the bit planes are equal in step 304, the next pixel is selected, as shown in step 306.

15 If the comparison does not yield a match, namely the bit planes are not equal in step 304, a second bit-wise comparison is made, of the 7th bit plane of the current frame with the 6th bit plane of the next frame, as in step 308.

20

If the second comparison yields a match, namely the bit planes are equal in step 310, a decision is made that tampering of this pixel occurred in the previous 'N-1' frame, as shown in step 314. If the comparison does not

25 yield a match, namely the bit planes are not equal in step 310, a decision is made that tampering of this pixel occurred in the current 'N' frame, as shown in step 312.

Furthermore, if an area is detected as having been
30 altered, for example by intentional tampering, it is within the contemplation of the invention that the area is visually labelled, as in step 316, to inform a user viewing the video of such tampering. The visual labelling

may take any form appropriate to make clear that tampering has occurred, which may include one or any combination of the following techniques:

(i) replacing any or all of the tampered image pixels with a known value. The known value is preferably selected to be sufficiently different from the source image content such that the tampering is clearly visible, for example black, white, any saturated colour, any non-natural colour;

(ii) altering only the coloured appearance of a tampered pixel such that the underlying image content remains visible but the tampering is clearly marked;

(iii) replacing only one component of a tampered pixel with a known value, for example 0 or 255, in an image format comprising more than one component;

(iv) visually labelling (using one or more of (i) or (ii) or (iii) above) the complete image frame within which any of the pixels are detected as having been tampered with and/or;

(v) visually labelling (using one or more of (i) or (ii) or (iii) above) the complete image frame, and all subsequent images in the video sequence, within and following an image frame in which any of the pixels are detected as having been tampered with.

Examples of 'watermarking' communication units suitable for incorporating the aforementioned inventive concepts are described in filed UK patent applications GB9914384.4 and GB0031085.4, to the present applicant, whose contents are contained herein by reference.

However, FIG. 4 describes a preferred configuration of video/image communication units to implement the preferred

12

embodiment of the present invention. Referring now to
FIG. 4, a video communication system 400 is shown, in
accordance with the preferred embodiment of the invention.
The video communication system 400 includes a transmitting
5   video/image communication unit 405 for embedding a
watermark, and a receiving video/image communication unit
450 for detecting a watermark.

The transmitting video/image communication unit 405,
10   includes a video/image input port 415 for receiving
video/image signals. A video/image signal is passed to
processor 410, which includes three watermark-embedding
processes.

15   A first selection function/algorithm 420 selects the
component in which to embed the tamper evidence.
A second selection function/algorithm 425 then selects the
region of the video/image in which to embed the tamper
evidence. The tamper evidence is then applied in
20   function/algorithm 430, in accordance with the method
described with respect to FIG. 1 and FIG. 2. The video
signal is then transmitted from transmitter 435 to the
receiving video/image communication unit 450.

25   It is within the contemplation of the invention that
alternative forms of moving video or image data may be
used, for example 'transmission' may take the form of
copying onto video tape, sending as an internet file,
copying onto a floppy disk etc.
30
The receiving video/image communication unit 450, includes
a receiver 455 for receiving video/image signals. A

received watermarked video/image signal is passed to
processor 460, which includes three watermark processes.

A first function/algorithm 465 applies the tamper
5   evidence, in accordance with the method described with
respect to FIG. 1 and FIG. 2. A second tamper detection
function/algorithm 470 then detects whether tampering
occurred, in accordance with the method described with
respect to FIG. 3. If tampering is detected, the
10 video/image signal is passed to a third visually labelling
function/algorithm 475, to label the tampered areas, prior
to passing the tampered signal to a display 480.

A benefit of the aforementioned inventive concepts is that
15 they can be readily implemented in existing video
communication units. More generally, the set of
algorithms used to effect the image frame/5th bit plane
manipulation and processing may be implemented in a
respective communication unit in any suitable manner. For
20 example, new apparatus may be added to a conventional
communication unit.

Alternatively existing parts of a conventional
communication unit may be adapted, for example by
25 reprogramming one or more processors 410, 460 therein. As
such the required adaptation may be implemented in the
form of processor-implementable instructions stored on a
storage medium, such as a floppy disk, hard disk,
programmable read only memory (PROM), random access memory
30 (RAM) or any combination of these or other storage
multimedia.

14

It will be understood that the video transmission and watermarking arrangements described above provide at least the following advantages:

(i) means for submission of video evidence to a court of

5   law for which it may be shown that the video has not been tampered with since initial acquisition and storage;

(ii) means for purchasers of video and image material to authenticate the material such that it has not been altered since initial acquisition and storage;

10   (iii) means for distributors of video and image material to verify that material passed to them for distribution is genuine and has not been tampered with since initial acquisition and storage; and

(iv) means for fraudulent tampering of images and video to

15   be detected, and the location of such tampering to be revealed to users of the material.

In summary, a video communication unit comprising a video input for receiving a video or image signal transmission

20   has been described. The video or image signal includes a number of video or image frames, wherein each video or image frame includes a number of bit planes. The video input is operably coupled to a processor that replicates at least one bit plane in at least two received video or

25   image frames to provide a means of tamper detection of the video or image signal transmission.

In addition, or in the alternative, a video communication unit has been described, for example the above video

30   communication unit, that includes a video receiver for receiving, from a transmitting video communication unit, a watermarked video signal transmission. The watermarked video signal transmission has a number of video or image

15

frames, wherein each video or image frame includes a
number of bit planes. The receiver is operably coupled to
a processor that compares at least one bit plane of at
least two subsequent video or image frames to detect any
5   tampering of the watermark.

In addition, or in the alternative, a video communication
unit, for example either of the above video communication
units, has been described that includes a processor that
10   detects tampering of an area of an image of a received
video or image transmission. The processor visually
labels, upon detection of said tampering, said area to
inform a user viewing the image or video of said tampering
of said video or image transmission. In such a case, it
15   is not essential that the aforementioned method of tamper
detection be used.

In the preferred embodiment of the invention, a mobile
radio device may incorporate any of the above video
20   communication units. The mobile radio device may be a
mobile phone, a portable or mobile PMR radio, a personal
digital assistant, a laptop computer or a wirelessly
networked PC. Further, a video transmission system
adapted to use any of the above video communication units
25   has been provided.

A method of watermarking a video signal transmission in a
video transmission system has also been described. The
method includes the steps of receiving a video or image
30   signal transmission that has a number of video or image
frames, wherein each video or image frame includes a
number of bit planes. The method also includes the step
of replicating at least one bit plane in a video or image

frame to provide a means of tamper detection of the video or image signal transmission.

Thus, a method of embedding a watermark in a video
5   sequence has been described that should be sufficient for evidentiary purposes of tampering, thereby improving upon the disadvantages with prior art arrangements.

In addition, or in the alternative, a method of detecting
10   tampering of a watermarked image, has been described. The method includes the steps of receiving a watermarked image that has a number of video or image frames, wherein each video or image frame includes a number of bit planes, at least one of which is watermarked. The method also
15   includes the steps of extracting said watermarked bit plane from a previous frame; and comparing said at least one watermarked bit plane in at least two subsequent video or image frames to detect any tampering.

20   In addition, or in the alternative, a method of visually labelling a video or image transmission has also been described. The method includes the step of altering a coloured appearance of a tampered pixel to inform a user viewing the video or image transmission of said tampering
25   of said video or image transmission. Again, in such a case, it is not essential that the aforementioned method of tamper detection be used.

In such a manner, the labelling method allows areas of a
30   video sequence to be highlighted that are detected as having been tampered with.

17

Claims

1. A video communication unit (405) comprising a video
input (415) for receiving a video or image signal

5   transmission having a number of video or image frames,
wherein each video or image frame (110, 120) includes a
number of bit planes (130-150), the video input (415)
being operably coupled to a processor (410), the video
communication unit (405) characterised by said processor

10   replicating at least one bit plane (140) in at least two
received video or image frames to provide a means of
tamper detection of the video or image signal
transmission.

15   2. The video communication unit according to claim 1,
wherein replication of at least one bit plane (140) in
subsequent video or image frames is made in consecutive
video or image frames.

20   3. The video communication unit according to claim 1 or
claim 2, wherein replication of at least one bit plane
(140) includes replicating a less significant bit plane of
a previous frame in a more significant bit plane (150) of
a current frame.

25

4. The video communication unit according to any preceding
claim, wherein replication of at least one bit plane (140)
is repeated throughout the video or image signal
transmission.

30

5. The video communication unit according to any preceding
claim, wherein replication of at least one bit plane (140)
includes replication of a subset of pixels within a frame.

18

6. A video communication unit (450), comprising a video receiver (455) adapted for receiving, from a transmitting video communication unit (405) according to any preceding

5   claim, a watermarked video signal transmission having a number of video or image frames (110, 120), wherein each video or image frame includes a number of bit planes (140, 150), the receiver being operably coupled to a processor (460), the video communication unit (450) characterised by

10 said processor (460) comparing at least one bit plane (140) of at least two subsequent video or image frames to detect any tampering of the watermark.

7. The video communication unit (450) according to claim

15 6, further characterised by said processor (460) locating a spatial and temporal position of the tampering as the video signal is being played by the video communication unit.

20 8. The video communication unit (450) according to claim 7, further characterised by said processor determining a frame position of the tampered frame (225) by comparing an appropriate bit plane of a current frame to an expected matching bit plane of a previous frame (302), wherein:

25   if said comparison shows equal bit planes (304), no tampering has occurred; or

      if said comparison shows unequal bit planes, a further comparison (308) is made between the current frame and the next frame such that:

30   if said comparison shows equal bit planes (310) the tampering occurred in the previous frame (314); or

      if said comparison shows unequal bit planes, the tampering occurred in the current frame (312).

19

9. A video communication unit (450) according to any of
claims 6 to 8, the video communication unit comprising a
processor (460) that detects tampering of an area of an

5   image, the video communication unit characterised by said
processor (460) visually labelling (475), upon detection
of said tampering, said area to inform a user viewing the
image or video of said tampering.

10   10. The video communication unit (450) according to claim
9, wherein said visual labelling (475) includes replacing
any or all of said tampered image or video with a known
value such that said tampering is visible, for example
black, white, any saturated colour, and/or any non-natural

15   colour.

11. The video communication unit (450) according to claim
9, wherein said visual labelling (475) includes altering
only a coloured appearance of a tampered pixel such that

20   an underlying image content remains visible but said
tampered area is marked.

12. The video communication unit (450) according to claim
9, wherein said visual labelling (475) includes replacing

25   one component of a tampered pixel with a known value in an
image format comprising more than one component.

13. The video communication unit (450) according to any of
claims 9 to 12, wherein a complete frame is visually

30   labelled (475) when any pixel within said frame is
detected as having been tampered with.

14. The video communication unit (450) according to claim 13, wherein said complete frame and all subsequent frames in a video sequence within and following a frame in which any pixel is detected as having been tampered with are
5 visually labelled.

15. The video communication unit (405, 450) according to any preceding claim, wherein the watermark is applied to at least one of the following image formats: YCbCr, RGB,
10 or any single component of an image format.

16. The video communication unit (405, 450) according to any preceding claim wherein a watermark is applied in a restricted area or region of an image, or throughout the
15 entire image.

17. A video transmission system (400) comprising a video communication unit (405, 450) in accordance with any of claims 1 to 16.
20

18. A mobile radio device comprising a video communication unit (405, 450) in accordance with any of claims 1 to 16.

19. The mobile radio device of claim 18, wherein the
25 mobile radio device is a mobile phone, a portable or mobile PMR radio, a personal digital assistant, a lap-top computer or a wirelessly networked PC.

20. A method of watermarking a video signal transmission in a video transmission system, the method comprising the step of:

receiving (415) a video or image signal transmission

5   having a number of video or image frames (110, 120), wherein each video or image frame includes a number of bit planes (140, 150);

the method characterised by the step of:

replicating at least one bit plane (140) in a subsequent

10 video or image frame to provide a means of tamper detection of the video or image signal transmission.

21. A method of watermarking a video signal transmission according to claim 20, wherein the step of replicating

15 includes replicating at least one bit plane (140) in a subsequent consecutive video or image frame.

22. A method of watermarking a video signal transmission according to claim 21, wherein the step of replicating

20 includes replicating a less significant bit plane (140) of a previous frame (110) to a more significant bit plane (150) of a current frame.

23. The method of watermarking a video signal transmission

25 according to any of claims 20 to 22, wherein the step of replicating is repeated throughout the video or image signal transmission.

24. The method of watermarking a video signal transmission

30 according to any of claims 20 to 23, wherein the step of replicating includes replicating a subset of pixels within a frame.

25. A method of detecting tampering of a watermarked
image, the method comprising the step of receiving (455) a
watermarked image having a number of video or image frames
(110, 120), wherein each video or image frame includes a

5   number of bit planes (140, 150), at least one of which is
watermarked in accordance with the method of any of claims
20-24, the method characterised by the steps of:
extracting (465) said watermarked bit plane (140) from a
previous frame (110); and

10   comparing said at least one watermarked bit plane (140) in
at least two subsequent video or image frames to detect
any tampering of the watermark (470).

26. The method of detecting tampering of a watermarked

15   image according to claim 25, wherein the step of comparing
includes comparing a bit plane on a previous frame with a
different bit plane on the current frame (302) on a pixel-
by-pixel basis.

20   27. The method of detecting tampering of a watermarked
image according to claim 25 or claim 26, the method
further characterised by the steps of:
determining a frame position of the tampered frame by
comparing an appropriate bit plane of the current frame to

25   an expected matching bit plane of the previous frame,
wherein:
if said comparison shows equal bit planes (304), no
tampering has occurred; or
if said comparison shows unequal bit planes (304), the

30   method is further characterised by the step of:
making a further comparison (308) between the current
frame and the next frame such that:

23

if said comparison shows equal bit planes (310) the
tampering occurred in the previous frame (314); or
if said comparison shows unequal bit planes (310), the
tampering occurred in the current frame (312).

5

28. A method of visually labelling (475) a video or image
transmission containing an attacked watermark, the method
comprising the steps of:
(i) detecting tampering (470) of an area of an image of a
10   received image or video transmission, using the method of
detecting tampering of a watermarked image of any of
claims 25 to 27; and
(ii) visually labelling (475) said area to inform a user
viewing the video of said tampering of said received image
15   or video transmission.

29. A method of visually labelling (475) a video or image
transmission according to claim 28, the method further
characterised by the step of:
20   altering a coloured appearance of a tampered pixel to
inform a user viewing the video or image transmission of
said tampering.

30. The method of visually labelling a video or image
25   transmission according to claim 29, wherein said visually
labelling (475) step includes the step of:
replacing any or all of a tampered image with a known
value such that tampering is visible, for example black,
white, any saturated colour, and/or any non-natural
30   colour.

31. The method of visually labelling a video or image
transmission according to claim 29, wherein said visually

24

labelling (475) step includes the step of altering only a coloured appearance of a tampered pixel such that an underlying image content remains visible but the tampering is marked.

32. The method of visually labelling a video or image transmission according to claim 29, wherein said visually labelling (475) step includes the step of:
replacing one component of a tampered pixel with a known value in an image format comprising more than one component.

33. The method of visually labelling a video or image transmission according to any of claims 29 to 32, wherein said visually labelling (475) step includes the step of:
visually labelling a complete image frame within which any pixel is detected as having been tampered with.

34. A storage medium storing processor-implementable instructions for controlling one or more processors (410, 460) to carry out the method of any of claims 20 to 33.

35. A video communication unit adapted to perform any of the method steps of any of preceding claims 20 to 33.

36. A mobile radio device comprising a video communication unit in accordance with claim 35.

37. The mobile radio device of claim 36, wherein the mobile radio device is a mobile phone, a portable or mobile PMR radio, a personal digital assistant, a lap-top computer or a wirelessly networked PC.
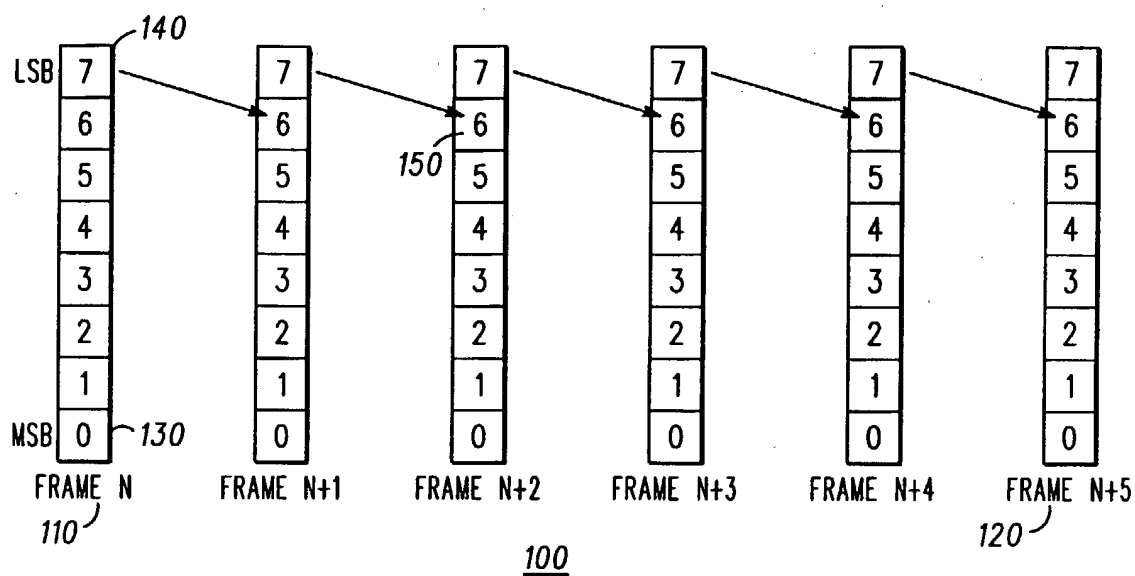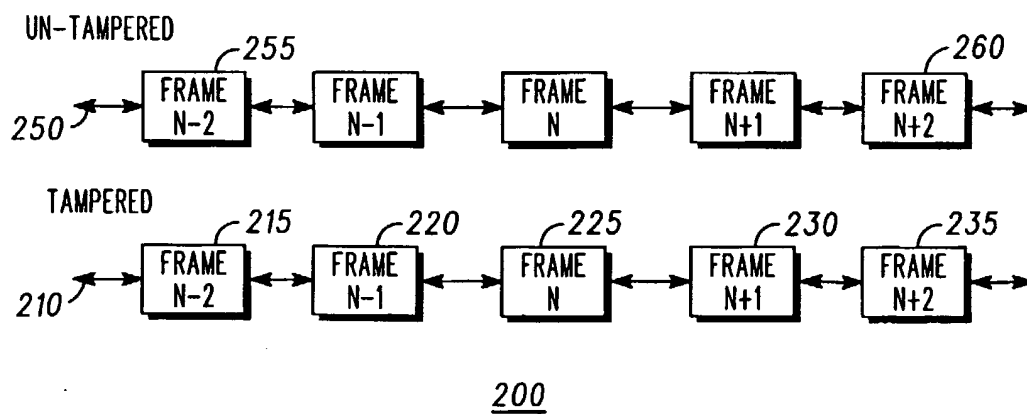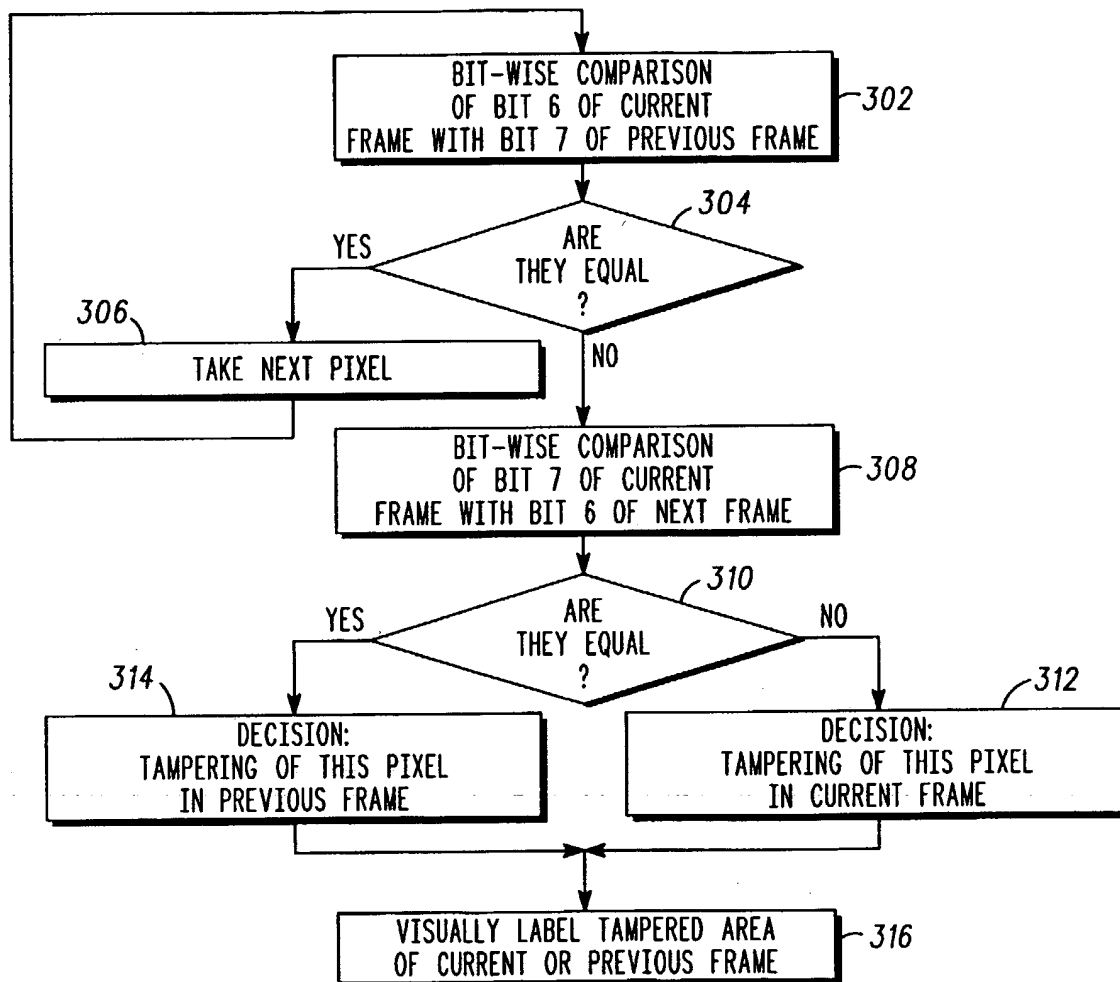
FIG. 1

FIG. 2

```
                    ┌──────────────────────────────┐
                    │      BIT-WISE COMPARISON      │
                    │       OF BIT 6 OF CURRENT     │──302
                    │ FRAME WITH BIT 7 OF PREVIOUS FRAME │
                    └──────────────────────────────┘
                                   │
                                   ▼
                                ╱     ╲   304
                       YES    ╱   ARE   ╲
          ┌──────────────────◁  THEY EQUAL ▷
          │                    ╲    ?    ╱
   306    │                      ╲     ╱
          │                         │ NO
   ┌──────▼──────────┐              │
   │  TAKE NEXT PIXEL │              ▼
   └─────────────────┘    ┌──────────────────────────────┐
                          │      BIT-WISE COMPARISON      │
                          │       OF BIT 7 OF CURRENT     │──308
                          │  FRAME WITH BIT 6 OF NEXT FRAME │
                          └──────────────────────────────┘
                                         │
                                         ▼
                                      ╱     ╲   310
                       YES          ╱   ARE   ╲          NO
            ┌────────────────◁  THEY EQUAL ▷────────────────┐
            │                   ╲    ?    ╱                   │
   314      │                     ╲     ╱                     │   312
   ┌────────▼──────────┐                         ┌────────────▼──────┐
   │    DECISION:       │                         │    DECISION:       │
   │ TAMPERING OF THIS PIXEL │                    │ TAMPERING OF THIS PIXEL │
   │  IN PREVIOUS FRAME │                         │  IN CURRENT FRAME │
   └───────────────────┘                         └───────────────────┘
            │                                                 │
            └───────────────────────┬─────────────────────────┘
                                     ▼
                    ┌──────────────────────────────┐
                    │ VISUALLY LABEL TAMPERED AREA  │──316
                    │  OF CURRENT OR PREVIOUS FRAME │
                    └──────────────────────────────┘
```

300

FIG. 3

3/3
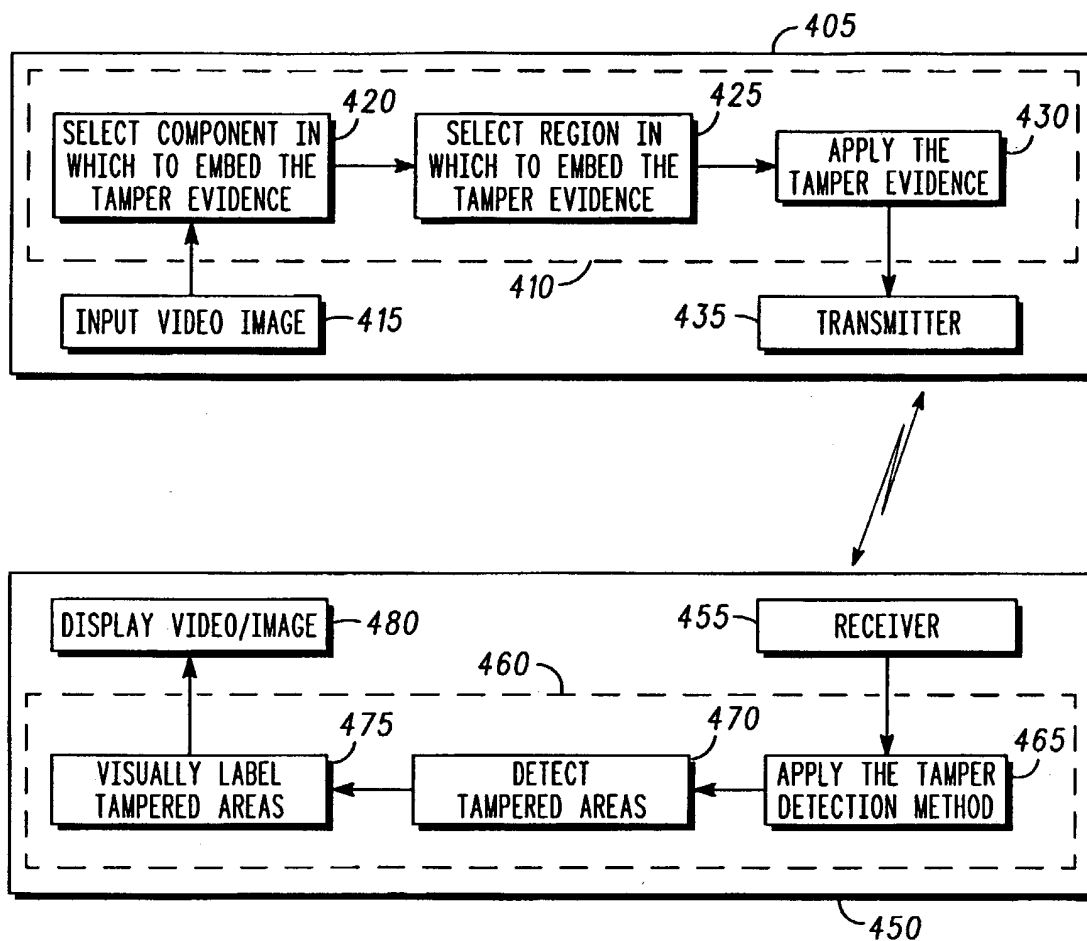
FIG. 4

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/24 G06T1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04N G06T

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MOBASSERI B G: "ORDERED BITPLANE WATERMARKING OF DIGITAL VIDEO BY DIRECT SEQUENCE SPREAD SPECTRUM" PROCEEDINGS OF INTERNATIONAL WORKSHOP ON MULTIMEDIA DATABASE MANAGEMENT, XX, XX, 5 August 1998 (1998-08-05), pages 66-71,ABSTRACT, XP000953697	1-5, 17-24, 34-37
Y	page 66, left-hand column, line 1 -page 66, right-hand column, paragraph 2 page 69, left-hand column, line 7 -page 69, right-hand column, last line	6-16, 25-33
Y	WO 00 64094 A (SIGNAFY INC) 26 October 2000 (2000-10-26) page 1, line 22 -page 1, line 33 page 4, line 7 -page 4, line 16 page 9, line 9 -page 9, line 21 page 11, line 1 -page 12, line 3	6-16, 25-33

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the International filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the International filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the International search	Date of mailing of the international search report
7 August 2002	19/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Schoeyer, M

Form PCT/ISA/210 (second sheet) (July 1992)

International Application No

PCT/EP 02/06670

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 953 938 A (HEWLETT PACKARD CO) 3 November 1999 (1999-11-03) column 2, line 36 -column 3, line 7 column 11, line 48 -column 12, line 17 ---	6-16, 25-33
A	HARTUNG F ET AL: "Digital watermarking of MPEG-2 coded video in the bitstream domain" ACOUSTICS, SPEECH, AND SIGNAL PROCESSING, 1997. ICASSP-97., 1997 IEEE INTERNATIONAL CONFERENCE ON MUNICH, GERMANY 21-24 APRIL 1997, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 21 April 1997 (1997-04-21), pages 2621-2624, XP010225693 ISBN: 0-8186-7919-0 page 2622, left-hand column, paragraph 2 -page 2622, right-hand column, paragraph 3 ---	1-33
A	WO 99 11020 A (DELP EDWARD J III ;GLOGAU JORDAN J (US); LIN EUGENE TED (US); PURD) 4 March 1999 (1999-03-04) page 1, line 12 -page 2, line 2 page 3, line 14 -page 3, line 30 page 7, line 20 -page 7, line 29 -----	1-33

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 0064094	A	26-10-2000	EP WO	1210789 A1 0064094 A1	05-06-2002 26-10-2000
EP 0953938	A	03-11-1999	US EP JP	2001046307 A1 0953938 A2 11355558 A	29-11-2001 03-11-1999 24-12-1999
WO 9911020	A	04-03-1999	WO	9911020 A1	04-03-1999